**Cybercriminals increasingly use online banking fraud automation techniques**

Cybercriminals have found a new way to perform online banking fraud. These attacks began in Europe and were reported in Italy, Germany, and the Netherlands. Recently, attacks have been made in Latin America and the U.S. as well. The attacks, labeled “Operation High Roller” by McAfee and Guardian Analytics researchers, have enabled cybercriminals to steal at least $75 million from high balance business and personal accounts. Researchers estimate that the attacks attempted to steal up to $2.5 billion. The attacks were made by combining traditional bank malware techniques with fraud automation techniques. The traditional malware allows the attacker to inject rogue content into online banking websites, which ultimately allows for the collection of financial details and log in credentials. Attackers then use server-hosted scripts to piggyback on active banking sessions. The scripts generated by the malware are designed for specific banking websites and automate the fraud process. By bypassing the banks two-factor authorization systems, attackers capture passwords generated by the bank issued token and performs the fraud in the background. Attackers gain access to the victim’s accounts and transfer out large sums of money, while a “please wait” message is displayed on the victim’s screen.

Despite apparent controls implemented by the banks, attackers were able to breach their security and steal millions of dollars. Attackers were able to overcome the two-factor authentication and gain access to passwords generated by bank issued tokens. As noted in the article, banks will have to be extremely aware of these attacks and take the appropriate measures to prevent this type of breach. Additionally, bypassing the two factor authentication means that there are security risks for other forms of physical security devices as well.